UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/810,354 | 03/16/2000 | Horst Henn | DE920000032US1 | 9201 |

7590 03/24/2004

Jeanine S. Ray-Yarletts
IBM Corporation
T81/062
P.O. Box 12195
Research Triangle Park, NC 27709

| EXAMINER | |
|---|---|
| JUNG, DAVID YIUK | |
| **ART UNIT** | **PAPER NUMBER** |
| 2134 | 4 |

DATE MAILED: 03/24/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/810,354 | HENN ET AL. | |
| | Examiner | Art Unit | |
| | David Y Jung | 2134 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *04 December 2001*.

2a)☒ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 March 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *3*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

### CLAIMS PRESENTED

Claims 1-15 are presented.

### CLAIM REJECTIONS

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Riggins et al. (cited by Applicant, International Publication Number WO 00/11832, hereinafter also referred as "Riggins").

Regarding claim 1, Riggins teaches "A security system for controlling access to one or more application functions located on a server or accessible via server, each application function having an associated security level, wherein one or more clients communicate with said server by means of requests for accessing one of said application functions using a network, wherein access to said application functions is controlled by security requirements (page 3, line 4 to page 4 line 2, global server handing requests for accessing applications), comprising:

an authentication component functionally separated from said clients and said application functions for processing said client request independently of said client type, containing more than one authentication mechanisms and selecting and executing an authentication mechanism from said more than one authentication mechanisms based on the information contained in the client request resulting in a security state (page 6, lines 20-29, the global server functionally separated from clients, and the global server providing authentication through firewall);

a security component containing a ... describing security requirements (security level) for accessing application functions, comparing said security state associated with said client with the security level of the application function and allowing access to the application function if the security state fulfills the security level (page 6, lines 20-29, global server providing security through firewall; page 3, line 19 to page 4 , line 2, multiples levels of authentication and multiple levels of resource access).

These passages of Riggins are not clear about a "security policy." A policy (in computer science) usually refers to a logical way of solving a problem. Riggins does discuss security levels being "enabled" -- page 3, line 19 to page 4 , line 2, multiples levels of authentication and multiple levels of resource access. "Enabling" usually refers a mechanism of physical (rather than logical) implementation.

Nevertheless, it was well known in the art to have a "security policy" (rather than predetermining a physical implementation) for the motivation of having flexibility in security.

It would have been obvious at the time of the claimed invention to combine "security policy" with the teachings of Riggins so as to teach the claimed invention for the motivation noted in the previous paragraphs.

Regarding claim 2 (wherein said clients are PVC-devices), Riggins suggests such (page 6, lines 16-19, wireless channel 146 permitting mobile access thereby suggesting PVC devices).

Regarding claim 3 (said authentication component and said security component are integrated in one component stored on a server), Riggins suggests such (global server being used for authentication and for security, as noted in the rejection of claim 1).

Regarding claim 4 (said authentication component consists of security plug-ins whereby each authentication mechanism is laid down in a separate security plug-in), Riggins suggests such (page 3, line 19 to page 4, line 2, multiple levels of resource access suggesting separate plug-ins).

Regarding claim 5 (whereby the authentication mechanism may be UserID/Password, Challenge/Response or digital signature), Riggins suggests such (page 3, line 19 to page 4, line 2, based on user status, suggesting such mechanism).

Regarding claim 6 (a component (ADL) for converting PVC-device specific requests into canonical requests before said request is used by said authentication component), Riggins suggests such (page 3, line 19 to page 4, line 2, global server using stored keys, suggesting canonical requests rather than device specific requests).

Regarding claim 7, Riggins teaches "A method for controlling access to one or more application functions stored on a server or accessible via server, each application function having an associated security level, wherein one or more clients communicate with said server by means of requests for accessing one of said application functions using a network, whereby access to said application functions is controlled by a security requirements (page 3, line 4 to page 4 line 2, global server handing requests for accessing applications), comprising the steps of:

... all incoming requests created by said clients to an authentication component which is functionally independent from said clients and saga application functions (page 6, lines 20-29, the global server functionally separated from clients, and the global server providing authentication through firewall), said authentication component comprising the steps of

authentication of said client by determining an authentication mechanism provided by said authentication component by means of authentication information contained in said request and applying said authentication mechanism; storing a result of said authentication and said authentication information or parts of it contained in said request as a security state; using security requirements for said one of said application functions to be accessed; comparing said stored security state with said security requirements for accessing the requested application function; and invoking said requested application function if said security state fulfills said security requirements (page 6, lines 20-29, the global server functionally separated from clients, and the global server providing authentication through firewall).

These passages of Riggins are not clear about a "routing." A routing (in computer science) usually refers to choosing among multiple paths between source and destination. Riggins does discuss global access – global server.

Nevertheless, it was well known in the art to have a "routing" for the motivation of providing a choice among paths (choices usually made on basis of traffic load or security).

It would have been obvious at the time of the claimed invention to combine "routing" with the teachings of Riggins so as to teach the claimed invention for the motivation noted in the previous paragraphs.

Regarding claim 8 (wherein said incoming requests are canonical requests), Riggins suggests such (page 3, line 19 to page 4, line 2, global server using stored keys, suggesting canonical requests rather than device specific requests).

Regarding claim 9 (said canonical requests are created by a Device Adaptation Layer which converts client specific requests into canonical requests), Riggins suggests such (page 3, line 19 to page 4, line 2, global server using stored keys, suggesting canonical requests rather than device specific requests).

Regarding claim 10 (comprising the further steps of:

creating a session identifier when establishing a communication between a client and a server and using said session identifier in all requests and responses between said client and said server), Riggins suggests such (page 3, line 19 to page 4, line 2, global server using stored keys when establishing communication channels, suggesting such session identifiers).

Regarding claim 11 (whereby said session identifier and said security state are placed in a cookie, whereby said cookie is inserted into each request and response between said client and said server), Riggins suggests such (page 3, line 19 to page 4, line 2, global server using stored keys when establishing communication channels, suggesting such session identifiers being placed in a storage such as a cookie – which is logical because Riggins uses the web)..

Regarding claim 12, (wherein said clients are PVC-devices), Riggins suggests such (page 6, lines 16-19, wireless channel 146 permitting mobile access thereby suggesting PVC devices).

Regarding claim 13 (A computer program comprising computer program code portions for performing respective steps of the method according to claim 7 to 12 when the program is executed in a computer), such programs are well known in the art for the motivation of implementing such methods on a computer.

Regarding claim 14 (A computer program product stored on a computer-readable media containing software code for performing of the method according to one of the claim 7 to 12 if the program product is executed on the computer), such products are well known in the art for the motivation of implementing such methods on a computer.

Regarding claim 15, Riggins teaches: A client-server system, wherein one or more clients, having client types, communicate with a server by means of requests for accessing application functions located on or accessible via said server, wherein access to said application functions is controlled by a security system located on said server

(page 3, line 4 to page 4 line 2, global server handing requests for accessing applications), wherein said security system comprises:

an authentication component, functionally separated from said one or more clients and said application functions for processing client requests independently of client type, containing one or more authentication mechanisms and selecting and executing an authentication mechanism from said authentication mechanisms based on the information contained in the client request, resulting in a security state (page 6, lines 20-29, the global server functionally separated from clients, and the global server providing authentication through firewall);

a security component containing a ... describing security requirements (security level) for accessing application functions, comparing said security state associated to a client with the security level of the application function and allowing access to the specified application function if the security state fulfills the security level (page 6, lines 20-29, global server providing security through firewall; page 3, line 19 to page 4 , line 2, multiples levels of authentication and multiple levels of resource access).

These passages of Riggins are not clear about a "security policy." A policy (in computer science) usually refers to a logical way of solving a problem. Riggins does discuss security levels being "enabled" -- page 3, line 19 to page 4 , line 2, multiples levels of authentication and multiple levels of resource access. "Enabling" usually refers a mechanism of physical (rather than logical) implementation.

Nevertheless, it was well known in the art to have a "security policy" (rather than predetermining a physical implementation) for the motivation of having flexibility in security.

It would have been obvious at the time of the claimed invention to combine "security policy" with the teachings of Riggins so as to teach the claimed invention for the motivation noted in the previous paragraphs.

***Conclusion***

The art made of record and not relied upon is considered pertinent to applicant's disclosure. The art disclosed general background.

***Points of Contact***

**Any response to this action should be mailed to:**

Commissioner of Patents and Trademarks

Washington, D.C. 20231

**or faxed to:**

(703) 746-7239, (for formal communications intended for entry)

**Or:**

(703) 746-5606 (for informal or draft communications, please label "PROPOSED" or "DRAFT")

Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington. VA., Sixth Floor (Receptionist).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to David Jung whose telephone number is (703) 308-5262 or Greg Morse whose telephone number is (703) 308-4789.

David Jung

---

Patent Examiner

2004-03-11